Using Common Criteria Protection Profiles

May 1999

By:
Gary Stoneburner
Computer Security Division, NIST
stoneburner@nist.gov, 301-975-5394

NIST United States Department of Commerce
National Institute of Standards and Technology

This presentation can be found at:
http://csrc.nist.gov/cc/info/grs_ppsum.pdf (PDF)
http://csrc.nist.gov/cc/info/grs_ppsum.ppt (PowerPoint)

What is the Common Criteria (CC)?

- International standard
  - CC Project (US, Canada, France, UK, Netherlands, Germany)
  - ISO 15408
- Dictionary of security requirements
  - Like an ala carte menu (with “dietary” suggestions)
- Includes description of PP, ST, and TOE
  - PP: Protection Profile = statement of need
  - ST: Security Target = description of IT meeting the need
  - TOE: Target of Evaluation = actual IT matching the ST

CC compared to TCSEC

- **TCSEC** (Orange book) = hierarchy of requirement sets
  - 6 Classes: C1, C2, B1, B2, B3, A1
  - Each class is a specific set of requirements
  - Incorporates specific policies
- **CC** = menu of requirements
  - **PP** = a specific requirement set
    - Built from the “menu”
    - Equivalent to a TCSEC class
    - Written as needed, to fit user need

What is a Protection Profile (PP)?

- A statement of user need
  - What the user wants to accomplish
  - A primary audience: mission/business owner
  - Also used by users, developers, evaluators, and auditors
- A system design document
  - Refines need through several levels into specific requirements
- A consistent thread from ‘what’ to ‘how’
  - Requirements match need in a manner the user can live with

Who ‘owns’ a PP?

- PP is fundamentally a statement of user need
- Ideally the ‘using’ community should own the PP and
  - Drive PP development
  - Soliciting input from developers, evaluators, auditors, and regulators
- User understands the mission/business and can state
  - what is expected of TOE
  - what is NOT expected of the TOE
- Others however ...
  - Vendors have a hard time stating what the product does NOT do
  - Security technical experts often fail to fully understand user needs

PP Outline

- INTRODUCTION
- TOE DESCRIPTION
- SECURITY ENVIRONMENT
- OBJECTIVES
- REQUIREMENTS
- RATIONALE

PP Outline (Continued)

- Introduction
  - Executive summary (what the owner of the money needs to see)
  - Clear statement of the security problem to be addressed
  - As far into the PP as many decision makers will ever go
- TOE Description
  - Adds greater detail to introduction
  - What is TOE and what is environment?
  - Targeted toward the technical manager

PP Outline (Continued)

- Security Environment
  - Address user concerns and facilitate requirement definition
  - Assumptions made in the development of this PP
    - Expectations on the environment that will not be addressed elsewhere
    - Expectations on the nature of the TOE (e.g., built from COTS)
    - Threats not covered due to explicit risk acceptance
  - Threats and organizational policies to be addressed
    - Those that are significant in terms of developing requirements
    - Those that PP users will want to see explicitly addressed
  - General level of assurance needed
    - Refinement of rest of PP to this point
    - Capture the gist of that is necessary to meet the PP goals

PP Outline (Continued)

- Objectives
  - How policies and threats will be addressed in light of assumptions
    - Nature of the requirements needed
    - Degree of effectiveness expected
    - Focus for efforts (prevent, detect, react, recover)
  - Relationship of objective to policy or threat
    - One to one, One to many, Many to one
    - Explicit and derived (implicit)

PP Outline (Continued)

- Requirements
  - Functions to be provided
    - Functions the TOE must provide
    - Functions the TOE’s environment must provide
      - Especially other IT than the TOE (important for composability)
    - Functions the TOE and its environment provide together
      - Some leeway in precisely what the TOE does
      - Desire to allow for some flexibility in the TOE design
  - Assurances that must be provided
    - Assurance = Grounds for confidence
    - Assurance = IT quality from a security perspective
    - Evaluator (or auditor) measures using PP as the yardstick
    - Ultimately assurance depends on the developer and operator

PP Outline (Continued)

- Rationale
  - Often packaged as a separate document
  - Shows why the PP is complete, correct, and internally consistent

How is “conformance” with PP Determined?

- Formal CC Project Recognition
- Private sector evaluation and validation
- Private sector assessment and validation
- Independent evaluation
- Vendor assertion
- Other ...

PP Conformance (Continued)

- Formal CC Project Recognition
  - PP, ST, and TOE all evaluated
    - Nationally accredited laboratories
    - Use internationally agree to evaluation methodology
    - Subjected to national scheme oversight
    - PP against CC, ST against PP, TOE against ST
  - Evaluated items receive national validation certificate
- Private Sector Evaluation and Validation
  - PP, then ST and TOE evaluated
    - Sector accredited laboratories (can be the national labs)
    - Sector agree to evaluation methodology
    - Sector oversight
  - Sector issues validation certificate

PP Conformance (Continued)

- Private sector assessment and validation
  - Sector determined assessment performed
    - Perhaps audit verses evaluation
    - PP might not be independently assessed
    - Sector determined assessment methodology
  - Sector issues validation certificate
- Independent evaluation
  - Sponsor selected laboratory (can be national lab)
  - Use methodology agree to between sponsor and lab
- Vendor assertion
  - IT developer claims compliance

Example of ‘PP’ Use - CS2

- Use by Washington, Utah, and Minnesota
- Specify requirements for ‘trustworthy IT’ portion of Certificate Authorities (CA) validation
- Form of use: Private sector assessment and validation
  - States selected CS2 as the requirement set, determining it to be correct and useful
  - System audit conducted by commercial audit firm
  - Auditing firms, with state guidance, determine audit methodology and hence the precise meaning of ‘CS2 compliance’
- CS2 can be found at: http://csrc.nist.gov/cc/pp/pplist.htm#CS2